Amendments to the Specification

Please replace paragraph [0021] with the following amended paragraph:

[0021] Referring now to FIG. 2, a table of a method for transferring information between an access point and a user station in accordance with one embodiment of the invention. In one embodiment of the invention, two parties or devices may establish communications with one anther in accordance with an IEEE 802.11 standard, which in one particular embodiment may be in accordance with an IEEE 802.11i standard, although the scope of the invention is not limited in this respect. For reference purposes herein, A may refer to access point 124 and S may refer to user station 110, although the scope of the invention is not limited in this respect. As shown in FIG. 2, during a probe response in which access point 124 may respond to a probe from user station 110, access point 124 may transmit a nonce, ANONCE, to user station 110 (AP → STA). In one embodiment of the invention, a nonce may be a value that is used in conjunction with a key and which may be utilized in rekeying. In one embodiment of the invention, a nonce may be used at most once, although the scope of the invention is not limited in this respect. In one embodiment of the invention, nonces may be random or pseudo-random values. As shown in FIG. 2, ANONCE may refer to the nonce of access point 124. In reply to the probe response, user station 110 may transmit the ANONCE and the nonce of the user station 110, SNONCE, back to access point 124, along with a first message integrity code (MIC1) in a process called a reassociate request (STA → AP). SNONCE may be random or pseudo-random as well. In response to a reassociate request received from user station 110, access point 124 may transmit the nonce of the user station 110, SNONCE, back to user station [[~~124~~]]110, along with a second message integrity code (MIC2) (AP → STA). The message integrity codes, MIC1 and MIC2, may be utilized to sign messages over an IEEE 802.11 channel, and may include HMAC-SHA-1, AES-CBC-MAC, and PMAC, or any other cryptographically secure message integrity code, although the scope of the invention is not limited in this respect.